P&I – 2014/2
v.1.0

België

Actualiteiten

Werkten mee aan ‘Actualiteiten’ voor België :

E. Kindt (EK), M. Y. S. Van Der Sype (YSVDS) en N. Vandezande (NV), onderzoekers, Interdisciplinary Center for Law & ICT - iMinds, KU Leuven, R. Saelens, (RS), onderzoeker Center for Law, Science, Technology & Society Studies (LSTS), Vrije Universiteit Brussel, en Bastiaan Bruyndonckx (BB), advocaat aan de balie te Brussel.

Coördinatie en editing : mr. E. Kindt

Internationaal

Rechtspraak

België veroordeeld wegens laattijdige nakoming Verordening biometrische paspoorten

De Europese Commissie verzocht het Hof van Justitie om zich te buigen over de inbreuk van België wegens nalatigheid om binnen de gestelde termijn biometrische paspoorten af te geven. Het gaat meer bepaald over de Verordening (EG) nr. 2252/2004 van 13 december 2004 betreffende normen voor de veiligheidskenmerken van en biometrische gegevens in door de lidstaten afgegeven paspoorten en reisdocumenten ("Verordening biometrische paspoorten"). Deze Verordening beoogt de harmonisatie van de veiligheidskenmerken, waaronder biometrische identificatiemiddelen, voor de paspoorten en reisdocumenten van de lidstaten. Artikel 1.2 stelde meer bepaald : ‘voor deze paspoorten en reisdocumenten wordt een opslagmedium gebruikt dat een gezichtsopname bevat. De lidstaten nemen ook vingerafdrukken in een interoperabel formaat op. (…) ’ .

Deze Verordening, aangenomen in 2004, legde de lidstaten op om biometrische paspoorten, ook met vingerafdrukken, uit te reiken ten laatste 36 maanden na het aannemen van de nodige technische specificaties. Deze specificaties werden door de Commissie uitgevaardigd bij Beslissing C(2006) 2909 van 28 juni 2006. Alle lidstaten moesten dus uiterlijk vanaf 29 juni 2009 biometrische paspoorten met vingerafdrukken uitreiken. Terwijl in België de foto reeds langer in de chip van het paspoort of reissdocument is opgeslagen, was dit nog niet het geval voor de vingerafdrukken. Op 11 september 2009 kondigde de Ministerraad de overheidsopdracht aan voor de uitrusting en bijhorende softwaren van alle biometrische loketten Andere lidstaten, waaronder Nederland, reiken het biometrisch paspoort, inclusief vingerafdrukken, al langer uit. In vele van die landen werd ondertussen een debat gevoerd

over de plaats van opslag van deze vingerafdrukken, ingezameld voor de aanmaak van de paspoorten. Nationale lidstaten bleven immers vrij om al dan niet te voorzien in een centrale opslag daarvan. De Verordening liet dit over aan de lidstaten. De mogelijke centrale opslag leidde in vele landen echter tot protest. Zo is men in Nederland voorlopig gestopt met de centrale opslag van de vingerafdrukken die werden afgenomen voor de paspoorten.

Niettegenstaande herhaalde aankondigingen in de media dat de biometrische paspoorten spoedig zouden verspreid worden, bleef België dus in gebreke. België betwistte dit dan ook voor het Hof niet. Over de precieze oorzaak van de laattijdigheid wordt weinig gecommuniceerd. Onenigheid met de vereniging voor beroepsfotografen evenals problemen bij de aanbesteding worden door sommigen zijdelings genoemd. Het Hof volstond met de vaststelling dat België zich aan het einde van de gestelde termijn bevond en derhalve haar verplichtingen heeft geschonden. Volgens sommige persberichten zouden de vingerafdrukken niet bewaard worden in een gegevensbestand (centrale opslag).

Eerder, in 2013, boog het Hof van Justitie – op verzoek van een Duitse rechtbank - zich reeds over de vraag of de overheid burgers wel mag verplichten om vingerafdrukken af te staan voor het aanvragen van een paspoort. In die zaak weigerde een Duitse advocaat, Michael Schwartz, om zijn vingerafdrukken af te geven bij de aanvraag van een nieuw paspoort wegens gebrek aan passende rechtsgrondslag en wegens schending van zijn grondrechten op gegevensbescherming en op privacy. Bij arrest van 17 oktober 2013 stelde het Hof dat het afnemen van vingerafdrukken wel degelijk het fundamenteel recht op eerbiediging van het privéleven en bescherming van persoonsgegevens schendt, maar dat deze schending gerechtvaardigd wordt door een erkende doelstelling van algemeen belang, met name het doel om de illegale binnenkomst van personen op het grondgebied van de Unie te voorkomen en om dus frauduleus gebruik van paspoorten tegen te gaan. De uitspraak is ook om nog andere redenen interessant. Het Hof stelde bijvoorbeeld ook dat de afname niet verder gaat dan noodzakelijk voor het verwezelijken van deze doelstelling. Ook wordt bevestigd dat de Verordening niet voorziet – zoals reeds onderstreept in punt 5 van de considerans van verordening nr. 444/2009 – en niet kan worden uitgelegd dat zij, als zodanig, een rechtsgrondslag biedt voor een eventuele centralisatie van verzamelde gegevens, of voor het gebruik van deze gegevens voor andere doeleinden dan dat van voorkoming van de illegale binnenkomst van personen op het grondgebied van de Unie. (overweging 61). Interessant is ook de overweging van het Hof dat vingerafdrukken een bijzondere rol vervullen op het gebied van de identificatie van personen in het algemeen, en meer in het bijzonder dat de vergelijking van de op een bepaalde plaats afgenomen vingerafdrukken met die welke worden bewaard in een database het mogelijk maakt om, hetzij in het kader van een crimineel onderzoek, hetzij met het oog op de uitoefening van indirect toezicht op een bepaalde persoon, de aanwezigheid van deze persoon op deze plaats vast te stellen (overweging 59). (EK)

Bronnen :

HvJ, 13 februari 2014, zaak C-139/13, Commissie tegen België; HvJ, 17 oktober 2013, zaak C-291/12, Michael Schwarz tegen Stadt Bochum, EHRC, 2014, afl. 1, p. 15, eveneens beschikbaar op

http://curia.europa.eu/juris/document/document.jsf?docid=143189&doclang=NL; zie ook X., 'Reispas aanvragen duurt dubbel zo lang door vingerafdrukken', Gazet van Antwerpen, 6.3.2014, beschikbaar op http://www.gva.be/nieuws/binnenland/aid1466462/reispas-aanvragen-duurt-dubbel-zo-lang-door-vingerafdrukken.aspx ; Buitenlandse Zaken, Buitenlandse Handel en Ontwikkelingssamenwerking, Biometrische paspoorten belangrijk middel in strijd tegen identiteitsfraude, 11.9.2009, beschikbaar op http://diplomatie.belgium.be/nl/Newsroom/Nieuws/Perscommuniques/buitenlandse_zaken/2009/september/ni_110909_biometrische_paspoorten.jsp

Privacy Algemeen

Regelgeving en beleid

Dashcams

Begin januari 2014 ontstond in België commotie over de publieke verspreiding van beelden van zogenaamde '*dashcams*'. Een *dashcam* wordt ook wel een *auto camera*, *dashboardcamera* of *carcam* genoemd. Een dashcam is een compacte videocamera die in de auto aan de voorruit wordt bevestigd en gedurende het traject het verkeer vóór de auto registreert.

De aanleiding van het publieke debat was een filmpje dat door de bestuurder van een bestelwagen werd gepost op Facebook en waarop te zien was hoe een bestuurder van een BMW de bestelwagen op de E314 rechts inhaalde en vervolgens, nadat de bestuurder van de bestelwagen met de lichten had geknipperd, tot drie maal toe bruusk remde zodat het bijna tot een aanrijding kwam. Het filmpje, waarop de nummerplaat van de BMW goed te zien was, werd in een mum van tijd duizenden malen gedeeld. De politie meldde daarop dat zij op basis van het filmpje een onderzoek zou instellen wegens verkeersagressie. Daarop barstte een publiek debat los over de wettigheid van het bewijs afkomstig van een dashcam en de vraag of het posten van een dergelijk filmpje op internet al dan niet een inbreuk op de privacy vormde.

De CBPL liet, bij monde van haar woordvoerster Eva Wiertz, weten te vrezen dat de man die met zijn dashcam het filmpje maakte en het op Facebook postte hiermee over de schreef was gegaan: "*Wie beelden maakt van iemand die een overtreding of een misdrijf pleegt, stapt met die beelden het best naar de politie. Die beslist dan, samen met het gerecht, wat er verder mee moet gebeuren. Maar zomaar iemand herkenbaar en zonder zijn toestemming op het net gooien, kan tot sancties leiden*".

De CBPL publiceerde vervolgens in januari 2014 op haar website een thema-artikel over dashcams. Daarin maakt zij een onderscheid tussen drie mogelijke scenario's.

Het eerste scenario is dat waarin de dashcam wordt gebruikt voor louter recreatieve doeleinden, bijvoorbeeld om het traject van een autovakantie te filmen. Als de beelden van deze autorit thuis worden opgeslagen en enkel en alleen worden gebruikt voor "*persoonlijke of huishoudelijke doeleinden*" (bv. het herbekijken van de beelden thuis of in familieverband)

zal de WVP niet van toepassing zijn. Zodra de beelden echter publiek worden gemaakt, zal de WVP wél van toepassing zijn en dient degene die de beelden publiek maakt de verplichtingen van de WVP na te leven. Hij zal beschouwd worden als een verantwoordelijke voor de verwerking. Als verantwoordelijke zal hij onder andere het proportionaliteitsbeginsel dienen te respecteren, moeten voldoen aan de informatieplicht, de nodige veiligheidsmaatregelen moeten nemen en een aangifte moeten verrichten.

Het tweede besproken scenario is dat waarbij de beelden van de dashcam worden gebruikt als bewijsmateriaal bij een aanrijding. In dit kader is er sprake van het gebruik van gerechtelijke persoonsgegevens, aldus de CBPL. De verwerking van dergelijke gerechtelijke persoonsgegevens is door de WVP in principe verboden, met dien verstande dat er op dit verbod enkele uitzonderingen bestaan. Een mogelijke uitzondering waarop men hier een beroep zou kunnen doen, is indien de verwerking "*noodzakelijk is voor het beheer van eigen geschillen*". In dit geval zou een dashcam mogelijk zijn, mits inachtneming van de verdere bepalingen van de WVP. Degene die de dashcam plaatst zal beschouwd worden als een verantwoordelijke voor de verwerking. Als verantwoordelijke zal hij onder andere het proportionaliteitsbeginsel dienen te respecteren (bv. de beelden 's avonds wissen als er overdag niets problematisch gebeurd is), moeten voldoen aan de informatieplicht (praktisch gezien zal dit bij een eerste contactname moeten gebeuren, bv. vlak na het ongeval als er met de tegenpartij wordt gesproken), de nodige veiligheidsmaatregelen moeten nemen en een aangifte moeten verrichten.

Het derde en laatste scenario betreft het gebruik van een dashcam in het interieur van een taxi. Als een taximaatschappij om veiligheidsredenen beslist om een camera in een taxi te installeren om het interieur te filmen (bijvoorbeeld om vandalisme of diefstal tegen te gaan of om de veiligheid van de chauffeur te verhogen), zal niet de WVP van toepassing zijn, maar wel de Wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's (de "Camerawet"). In overeenstemming met de Camerawet wordt een dergelijke camera beschouwd als een vaste bewakingscamera in een voor het publiek toegankelijke besloten plaats. De voornaamste verplichtingen zijn het plaatsen van een pictogram om passagiers in te lichten over de camerabewaking en het verrichten van een aangifte bij de CBPL. (BB)

Bronnen: *De Standaard, "Twijfels over bewijslast filmpje wegpiraat", zie http://www.standaard.be/cnt/dmf20140107_00916159*

CBPL, "Dashcams", zie http://www.privacycommission.be/nl/dashcams

Rechtspraak

Hof van Cassatie: Opname van telefoongesprek voor bewijsvoering niet strijdig met grondrechten

Op 8 januari 2014 oordeelde het Belgische Hof van Cassatie dat de persoon aan wie tijdens verscheidene telefoongesprekken criminele feiten worden onthuld, het recht heeft deze uitlatingen te registreren om zich er het bewijs van te verschaffen op het moment dat hij er bericht van geeft aan het openbaar ministerie.

Artikel 314*bis* van het Belgische Strafwetboek, alsook artikel 124 van de Wet Elektronische Communicatie, voorziet in een principieel verbod op registratie en kennisname van elektronisch gecommuniceerde informatie door zij voor wie de communicatie niet persoonlijk was bestemd. Het is m.a.w. verboden privécommunicatie of –telecommunicatie waaraan men niet deelneemt op te nemen of te registreren, tenzij alle deelnemers aan de communicatie hiermee hebben ingestemd.

Artikel 90*ter* en artikel 90*decies* van het Wetboek van Strafvordering bieden een uitzondering op dit principieel verbod voor wat betreft het 'gerechtelijk afluisteren'. Nochtans is deze uitzondering in het besproken geschil niet van toepassing, daar de registratie van de uitlatingen niet door een onderzoeksrechter waren bevolen, maar door de betrokkene zelf waren geïnitieerd.

Het Hof concludeert dat noch de artikelen 6 en 8 van het Verdrag van de Rechten van de Mens, noch artikel 314*bis* van het Strafwetboek verbiedt gebruik te maken van zulke registratie ten behoeve van bewijsvoering, door de persoon die, bij het kennisnemen van een crimineel feit of een misdrijf, ook daadwerkelijk voldoet aan de verplichting tot kennisgeving aan de procureur des Konings (YSVDS).

Bronnen: Cass. AR P.13.1935.F, 8 januari 2014 (http://justitie.belgium.be/nl/binaries/P131935F_tcm265-240402.pdf).

Bescherming Persoonsgegevens

Regelgeving en beleid

Uitbreiding Bevoegdheden Vlaamse Toezichtscommissie

Bij Decreet van 6 december 2013 houdende wijziging van het Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, wat de vaststelling van de toezicht- en handhavingsbevoegdheden van de Vlaamse toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer ("**VTC**") betreft, werden de bevoegdheden van de VTC uitgebreid.

Ter herinnering, de Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer werd opgericht bij Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer en is op Vlaams niveau bevoegd voor de zaken waarvoor de CBPL op federaal niveau bevoegd is.

De bevoegdheden van de VTC waren tot op heden van vierderlei aard.

Ten eerste verleent de VTC, op verzoek of op eigen initiatief, advies aan het Vlaams Parlement, de Vlaamse Regering, de instanties en belanghebbenden over de bescherming van de persoonlijke levenssfeer in het kader van het Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer en de uitvoeringsbepalingen ervan. De VTC wekt hiervoor nauw samen met de CBPL.

Ten tweede verleent de VTC machtigingen voor de elektronische mededeling van persoonsgegevens door een Vlaamse overheidsinstantie en dit binnen de zestig (60) dagen na de aanvraag en mits alle daartoe noodzakelijke gegevens aan de VTC zijn meegedeeld. De machtigingen die de VTC verleent, zijn openbaar. Op federaal niveau is het de CBPL, en meer bepaald het Sectoraal Comité voor de Federale Overheid, die dergelijke machtigingen verleent.

Ten derde dient de VTC advies te verstrekken alvorens de Vlaamse Regering een gegevensbron die persoonsgegevens bevat als een authentieke gegevensbron erkent.

Ten vierde dient de VTC in bepaalde gevallen een gunstig advies te verstrekken alvorens instanties een veiligheidsconsulent kunnen aanstellen.

De VTC brengt jaarlijks bij het Vlaams Parlement schriftelijk verslag uit over de vervulling van haar opdrachten gedurende het voorbije jaar, met inbegrip van aanbevelingen voor de toepassing van het Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer. Het verslag van de VTC wordt door het Vlaams Parlement openbaar gemaakt. De voorzitter van de VTC kan al dan niet op eigen verzoek op elk moment door het Vlaams Parlement worden gehoord.

Tot voor kort beschikte de VTC niet over een echte controlebevoegdheid voor de door haar te machtigen mededelingen van persoonsgegevens. Het Decreet van 6 december 2013 houdende wijziging van het Decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, wat de vaststelling van de toezicht- en handhavingsbevoegdheden van de VTC betreft, brengt daar echter verandering in.

Vanaf de inwerkingtreding, op 24 januari 2014, krijgt de VTC ook toezichts- en handhavingsbevoegdheden.

De VTC zal dan ook bevoegd zijn om (a) beveiligingsmaatregelen op te leggen wanneer een elektronische mededeling van persoonsgegevens aanleiding geeft tot een schending van de persoonlijke levenssfeer, (b) de aanpassing, de opschorting of de stopzetting te bevelen van de elektronische mededeling van persoonsgegevens waarvoor op grond van het Decreet een machtiging moet worden verleend, en die zonder machtiging gedaan wordt of die niet conform de voorwaarden of de termen van een machtiging uitgevoerd wordt, en (c) een onderzoek ter plaatse uit te voeren waarvoor een aantal bevoegdheden worden toegekend. Wie weigert zijn medewerking te verlenen aan de uitoefening van de toezichtbevoegdheden van de VTC, kan strafbaar worden gesteld.

De leden van de VTC en van het secretariaat van de VTC die bij de uitvoering van een onderzoek ter plaatse kennis krijgen van een misdrijf met betrekking tot de persoonlijke levenssfeer, zijn verplicht dat te melden aan de CBPL. Op deze manier beschikt de VTC

voortaan over meer armslag om haar toezicht op de machtigingsplicht nog efficiënter te kunnen uitoefenen. (BB)

Bronnen: Decreet van 6 december 2013 houdende wijziging van het decreet van 18 juli 2008 betreffende het elektronische bestuurlijke gegevensverkeer, wat de vaststelling van de toezicht- en handhavingsbevoegdheden van de Vlaamse toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer betreft, *BS* 14 januari 2014

CBPL, "*Uitbreiding bevoegdheden VTC*", zie http://www.privacycommission.be/nl/uitbreiding-bevoegdheden-vtc

Website Vlaamse Toezichtcommissie voor het elektronische bestuurlijke gegevensverkeer, zie http://vtc.corve.be/index.php

Campagne Kif Kif tegen racisme via sociale media

Kif Kif, een interculturele beweging voor gelijkheid en tegen racisme, lanceerde op 3 februari 2014 een nieuwe campagne om racisme op sociale media netwerken aan te kaarten. Hoewel er bij het Centrum voor Gelijke Kansen, de overheidsinstantie inzake racismebestrijding, in 2012 al 287 dossiers liepen tegen racistische opmerkingen op het internet, zogenaamde 'cyberhate', is Kif Kif van mening dat een meer grootschalige actie nodig is tegen dergelijke situaties. Met deze campagne wordt een nieuw platform gelanceerd, Wipe, waarop racistische uitlatingen gemeld en gebundeld kunnen worden. Wanneer een internetgebruiker geconfronteerd wordt met racistische uitlatingen, bijvoorbeeld op sociale media netwerken, zou dit via de Wipe applicatie aan Kif Kif gemeld kunnen worden. Wanneer medewerkers van de organisatie vaststellen dat het daadwerkelijk om racisme zou gaan, zouden screenshots van de uitlatingen – samen met de gebruikersnaam van de betrokkenen – gepubliceerd worden op Wipe. Het doel van deze publieke schandpaal is volgens Kif Kif het in kaart brengen van de precieze schaal van online racisme. Ook kunnen dergelijke gevallen na beoordeling door het team achter Wipe doorgestuurd worden naar de bevoegde instanties, zoals het Centrum voor Gelijke Kansen. Met Wipe is het de bedoeling de drempel te verlagen om effectief online racisme aan te klagen. Anderzijds wordt gehoopt dat de campagne ook sensibiliserend zou werken.

Het publieke karakter van de campagne stuitte echter al snel op verzet. Zo werd reeds aangehaald dat de campagne het recht op vrije meningsuiting zou miskennen, alsook dat het een inbreuk zou uitmaken op de privacy van de betrokkenen. De vrije meningsuiting zou volgens Kif Kif niet in het gedrang zijn wanneer het gaat om strafbare feiten zoals aanzet tot haat, discriminatie en geweld. Ook wat privacy betreft, ziet Kif Kif geen graten in de campagne. Gezien de berichten die op Wipe gepubliceerd worden afkomstig zijn van publieke fora zoals sociale netwerken, is er volgens Kif Kif immers geen inbreuk op de privacy. Hier moet echter worden opgemerkt dat de publicatie van een bericht op een platform zoals Wipe wellicht niet als verenigbaar beschouwd kan worden met het

oorspronkelijke doel waarmee dergelijke berichten op openbare fora zoals sociale netwerken geplaatst werden. Bijgevolg kan de campagne wel beschouwd worden als een inbreuk op de bescherming van de persoonsgegevens van de betrokkenen. Dit punt werd ook aangehaald door de CBPL, die publiek reageerde op het voorval en contact opnam met Kif Kif. Daarnaast wordt aangeraden dergelijke zaken aan bevoegde instanties over te laten. De screenshots zijn intussen verwijderd, maar het is wel nog mogelijk om meldingen in te dienen via Wipe. (NV)

Bronnen: Y. Delepeleire, L. Louage, "Kif Kif verwijdert screenshots 'racistische taal' van site", De Standaard 3 februari 2014; Kif Kif, "[Persbericht] Kif Kif lanceert wipe: The Wiper kondigt de antiracistische strijd 2.0 aan", <www.kifkif.be>*.*

Bedrijfsleven

Regelgeving en beleid

Advies CBPL betreffende het eRegister van Wegvervoersondernemingen

De Europese Verordening 1071/2009 van 21 oktober 2009 tot vaststelling van gemeenschappelijke regels betreffende de voorwaarden waaraan moet zijn voldaan om het beroep van wegvervoerondernemer (de 'Verordening') uit te oefenen stelt dat elke Lidstaat een nationaal elektronisch register moet bijhouden van alle wegvervoersondernemingen die een vergunning verkregen hebben voor de uitoefening van dat beroep. Gezien dergelijk register onvermijdelijk ook persoonsgegevens zou bevatten, gaf de EU al aan dat elke verwerking van dergelijke gegevens in overeenstemming moet gebeuren met de Privacyrichtlijn. België nam in 2011 al stappen om deze verordening in nationaal recht om te zetten. Een eerste wetsontwerp werd negatief onthaald door de CBPL in haar advies 14/2011. Een herwerkte versie werd in het advies 17/2011 echter wel gunstig ontvangen. Toch zou het nog tot 15 juli 2013 duren vooraleer de uiteindelijke wet betreffende het eRegister van wegvervoersondernemingen – of de wet eRegister – aangenomen zou worden. Daarna zou het nog tot 18 februari 2014 duren vooraleer de wet gepubliceerd werd in het Belgisch Staatsblad. Hiermee is de lange weg van deze wet echter nog niet ten einde: de inwerkingtreding van de wet eRegister dient te worden bepaald door middel van Koninklijk Besluit. In haar advies 06/2014 van 5 februari 2014 analyseert de CBPL het ontwerp voor dergelijk Koninklijk Besluit.

De wet eRegister regelt de oprichting van het door de EU opgelegde elektronisch register van wegvervoersondernemingen. Wat de bescherming van persoonsgegevens betreft, duidt de wet een verantwoordelijke voor de verwerking aan. Ook bevat de wet bepalingen betreffende de doeleinden waarvoor de gegevens uit het register gebruikt kunnen worden, de authentieke bron, en dergelijke. Het Koninklijk Besluit wil hoofdzakelijk de op te nemen gegevens verder preciseren, wijzigen en aanvullen, de authentieke bronnen aanduiden, en

de gevallen aanduiden waar geen voorafgaande machtiging door het bevoegde sectoraal comité vereist is voor de raadpleging van het register.

Wat de op te nemen gegevens betreft, worden negen categorieën van gegevens bepaald, krachtens de minima opgelegd door de Verordening. De CBPL stelt voor om dergelijk onderscheid verder uit te werken in een tabel als bijlage bij het besluit. Hoewel het ontwerp van besluit een informatieplicht oplegt, herhaalt de CBPL dat de informatieplicht uit de Privacywet ruimer is. Door de informatieplicht te splitsen over de wet eRegister en het uitvoerend besluit van die wet, terwijl daarenboven ook nog de algemene Privacywet van toepassing blijft, stelt zich mogelijks het risico dat deze plicht niet correct wordt uitgevoerd. Zo vermeldt het besluit ook een toegangsrecht, dat echter nauwer is dan het algemene toegangsrecht uit de Privacywet. Een rechtstreekse verwijzing naar de Privacywet zou daarom wenselijker zijn. Waar de Verordening een minimale bewaartermijn van twee jaar voorstelt, legt het ontwerp van besluit een maximale termijn van 10 jaar op, te rekenen vanaf de dag dat de vervoerswerkzaamheden van de betrokken persoon beëindigd werden.

De toegang tot het eRegister vereist in principe voorafgaande machtiging van het sectoraal comité federale overheid. Echter legt de Verordening de openbaarmaking van een aantal gegevens op, mits respectering van de relevante bepaling inzake de bescherming van persoonsgegevens. Hier gaat het dan bijvoorbeeld om de naam en adres van de vervoersonderneming, alsook de aard van de vergunning. De CBPL herinnert eraan dat dergelijke publiciteit met het oog op transparantie geen afbreuk doet aan verplichtingen betreffende het hergebruik van de betrokken persoonsgegevens. Gezien hier in principe de toestemming van de betrokkene vereist is, en deze ook een recht van verzet heeft, wordt aangeraden deze punten op te nemen in het ontwerp van besluit. Ook wordt geadviseerd de openbaarmaking te beperken, om het risico van disproportionele publiciteit te vermijden. Gelijkaardige bedenkingen gaan op bij de mogelijkheid tot raadplegen van de kentekenplaat van de vergunde voertuigen. Hoewel politiediensten hier toegang toe moeten krijgen, moet hier benadrukt worden dat dergelijke toegang slechts beperkte doelen dient. Tot slot voegt het ontwerp van besluit nog een aantal gevallen toe waar geen voorafgaande machtiging vereist is.

De CBPL ziet geen fundamentele tekortkomingen in het ontwerp van besluit, maar raadt toch aan een aantal verduidelijkingen op te nemen om de correcte toepassing van de Privacywet te garanderen. (NV)

Bron: CBPL, "Advies 06/2014 van 5 februari 2014 betreffende het Ontwerp van Koninklijk Besluit betreffende het eRegister van Wegvervoersondernemingen", <www.privacycommission.be>, *11 p.*

Centraal aanspreekpunt voor Belgische fiscus binnenkort operationeel

Vanaf 1 mei 2014 is informatie van alle bankrekeningen van alle Belgen gecentraliseerd in het zogenoemde Centraal Aanspreekpunt (CAP) bijgehouden door de Nationale Bank. Banken dienen hiertoe informatie over de identiteit van hun klanten en hun rekeningnummers aan de Nationale Bank over te maken. Zodoende kan de fiscale

administratie gemakkelijker te weten komen bij welke financiële instelling de cliënt zijn rekeningen heeft. Dit is veel handiger – mede in het licht van de opheffing van het bankgeheim sinds 2011- dan elke bank aan te schrijven met de vraag of een 'verdachte' belastingplichtige bij die instelling een rekening heeft. Ook het bestaan van sommige contracten, waaronder alle mogelijke vormen van kredietverlening (hypothecaire lening, kredietopening, consumentenkrediet...) boven het bedrag van 200 euro, en leasingcontracten en overeenkomsten met betrekking tot beleggingsactiviteiten dienen doorgegeven te worden. Filialen of verkooppunten van buitenlandse financiële instellingen en leasingondernemingen of beleggingsvennootschappen moeten eveneens aan de meldingsplicht voldoen. De banken hebben de opdracht om alle gegevens vanaf 2010 door te geven.

Het CAP wordt opgericht en geregeld via een koninklijk besluit van 17 juli 2013 (B.S. 26.7.2013). De bedragen of beleggingen op een rekening worden niet meegedeeld aan het CAP. Het CAP zal onder voorwaarden elektronisch kunnen geraadpleegd worden door belastinginspecteurs, als er een duidelijk vermoeden van fiscale fraude bestaat, evenals bij een taxatie op basis van 'tekenen en indiciën'. De belastingplichtige zal wel vooraf moeten gewaarschuwd worden teneinde de mogelijkheid te hebben zich te verdedigen. Elke belastingplichtige mag eveneens zijn gegevens inkijken die het CAP op zijn naam bewaart. Dat kan via schriftelijke aanvraag aan de Nationale Bank van België. Bij de aanvraag dient een kopie van de identiteitskaart gevoegd te worden. De belastingplichtige kan eveneens kosteloos de rechtzetting of verwijdering vragen van onjuiste gegevens die het CAP op zijn naam bewaart. (EKI)

Bronnen : Koninklijk besluit van 17 juli 2013 (B.S. 26.7.2013)

Rechtspraak

Overheid

Regelgeving en beleid

Politioneel informatiebeheer hervormd

Op 6 februari 2014 is het wetsontwerp betreffende de wijziging van de Wet van 5 augustus 1992 op het politieambt in de Senaat aangenomen. De Kamer had dit al eerder gedaan op 18 november 2013. De wijzigingen van de Wet op het politieambt hebben betrekking op het politionele informatiebeheer (artikel 44/1 tot en met artikel 44/11 oud). Een hervorming van het hoofdstuk in de Wet op het politieambt inzake het politionele informatiebeheer heeft ongeveer 10 jaar op zich laten wachten. Niet dat er geen werk werd gemaakt van een herziening van de wet. Alleen konden de ingediende initiatieven niet de democratische toets doorstaan.

Artikel 44/1 vormde louter een algemeen wettelijk kader voor de verwerking van persoonsgegevens binnen het kader van bestuurlijke en gerechtelijke opdrachten. De uitvoering ervan werd echter geregeld via een ministeriële omzendbrief (de gemeenschappelijke richtlijn MFO-3 van 14 juni 2002 van de Ministers van Binnenlandse Zaken en Justitie betreffende het informatiebeheer inzake gerechtelijke en bestuurlijke politie). Deze omzendbrief wordt nu in de Wet op het politieambt opgenomen. Zo bestond er geen specifieke regeling voor de opslag van informatie in de Algemene Nationale Gegevensbank (ANG), noch voor de bijzondere gegevensbanken die regionaal en lokaal worden gebruikt. Nu legt de nieuwe wet de voorwaarden voor het aanleggen van gegevensbanken vast, zegt wie daarvoor verantwoordelijk is en welke gegevens in de ANG moeten opgenomen worden. Daarnaast worden per categorie persoonsgegevens bewaartermijnen vastgelegd, inclusief de termijnen waarbinnen deze gegevens kunnen geraadpleegd worden. Even belangrijk is de plicht van de politie om zo nodig de persoonsgegevens recht te zetten. Bijgevolg zal de politie voortaan automatisch onjuiste gegevens moeten verbeteren. Tegelijk krijgt de burger het recht om rechtzetting van zijn persoonsgegevens te vragen. Op die manier wil de wetgever voorkomen dat, wanneer iemand onschuldig is, zijn gegevens onterecht in de ANG bewaard blijven. Daarentegen kan de burger geen rechtstreekse inzage uitoefenen. Om het recht op inzage uit te oefenen, moet de burger zich nog steeds wenden tot de Commissie voor de Bescherming van de Persoonlijke Levenssfeer (CBPL). De CBPL kan dan nagaan of de betrokkene op wettige wijze in de ANG (of andere politionele databank) is geregistreerd. Is dat niet het geval, dan moeten de gegevens gewijzigd of vernietigd worden.

Ten opzichte van de oude regeling van het politionele informatiebeheer, is de nieuwe regeling in ieder geval een goede stap voorwaarts. Zo wordt het begrip “concreet belang” uit artikel 44/1 geschrapt en wordt de term “toereikend en ter zake dienend en niet overmatig” ingevoerd. Daardoor wordt van de politieman een extra inspanning gevraagd bij de vraag of bepaalde informatie van de burger in de politionele databank kan opgeslagen worden. Het is afwachten hoe dat in de praktijk zal uitgevoerd worden. Wellicht wordt een en ander nog geconcretiseerd via ministeriële omzendbrieven.

Toch blijven bepaalde aspecten onduidelijk. Dat is met name het geval ten aanzien van de gegevensoverdracht naar externe partners (binnen- en buitenland) en de doorstroming van gerechtelijke informatie naar bestuurlijke overheden. Niet helder is hoe de uitwisseling van politionele informatie verloopt in verband met de internationale verplichtingen inzake politionele samenwerking. Daarnaast worden de andere bestemmelingen van politionele informatie in een uitvoeringsbesluit vastgelegd. Merken we op dat dit reeds het geval was onder de oude regeling. Tot nog toe werd nooit zo’n uitvoeringsbesluit uitgebracht. En toch wordt politionele informatie van “andere” overheden gedeeld. (RS)

Bron: Wetsontwerp betreffende het politionele informatiebeheer en tot wijziging van de wet van 5 augustus 1992 op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens en het Wetboek van Strafvordering (Parl. St. Kamer, nr. 53-3105), www.dedamer/documenten.be.

Zorg en Welzijn

Regelgeving en beleid

Rechtspraak

Arbeid

Regelgeving en beleid

Rechtspraak

Bookmark

Agenda